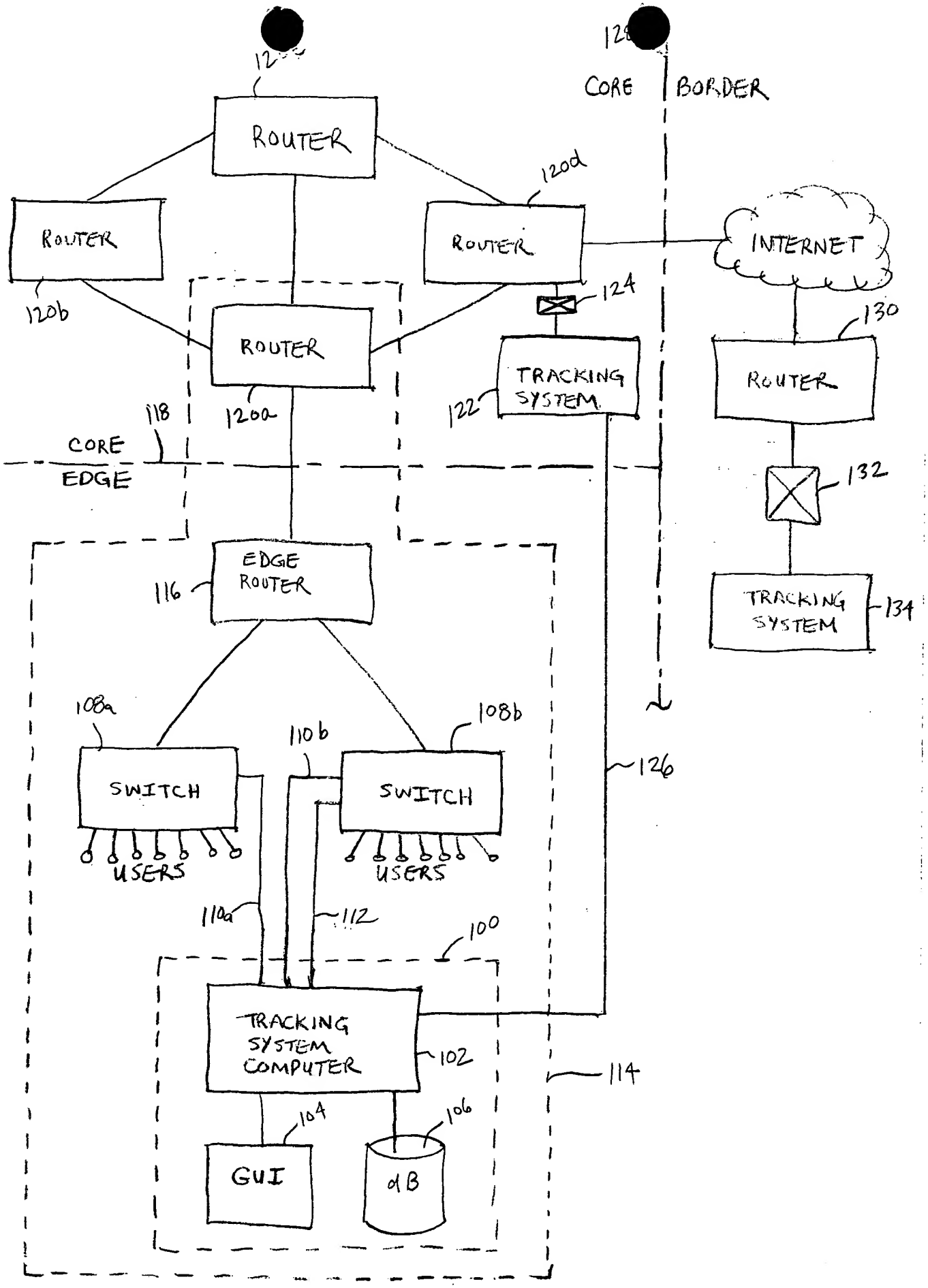
CORE
BORDER
ROUTER
ROUTER
ROUTER
ROUTER
ROUTER
INTERNET
TRACKING SYSTEM
ROUTER
TRACKING SYSTEM
CORE
EDGE
EDGE ROUTER
SWITCH
SWITCH
USERS
USERS
TRACKING SYSTEM COMPUTER
GUI
dB
120b
120a
120d
124
122
130
132
134
118
116
108a
108b
110b
110a
112
100
102
104
106
114
126

FIG. 1

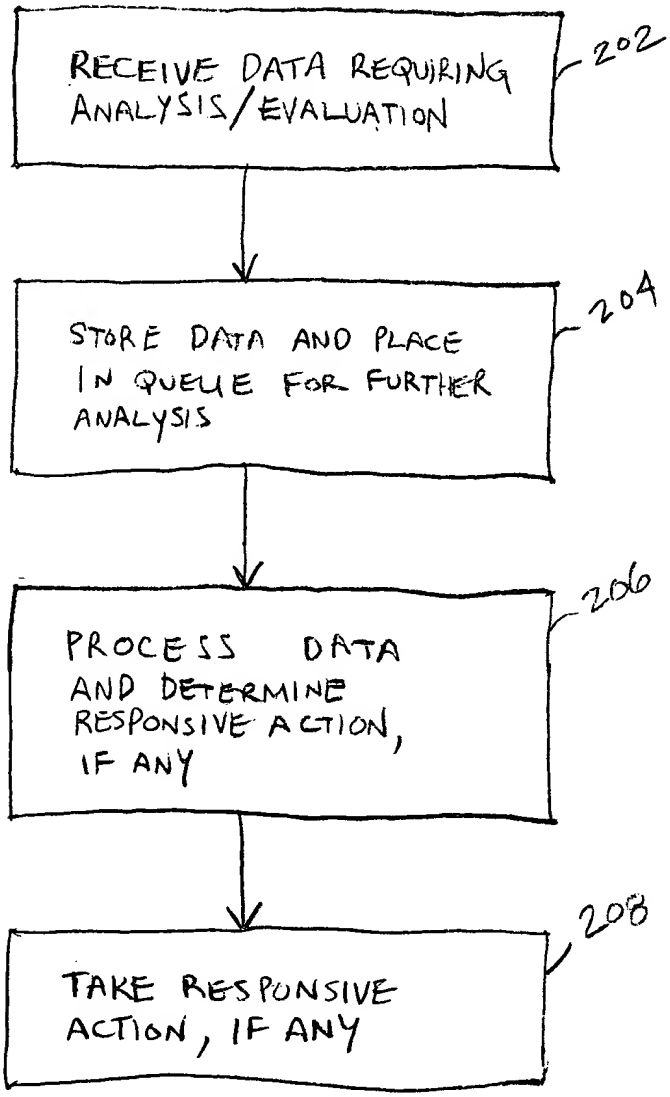
RECEIVE DATA REQUIRING ANALYSIS/EVALUATION
202
STORE DATA AND PLACE IN QUEUE FOR FURTHER ANALYSIS
204
PROCESS DATA AND DETERMINE RESPONSIVE ACTION, IF ANY
206
TAKE RESPONSIVE ACTION, IF ANY
208

FIG. 2

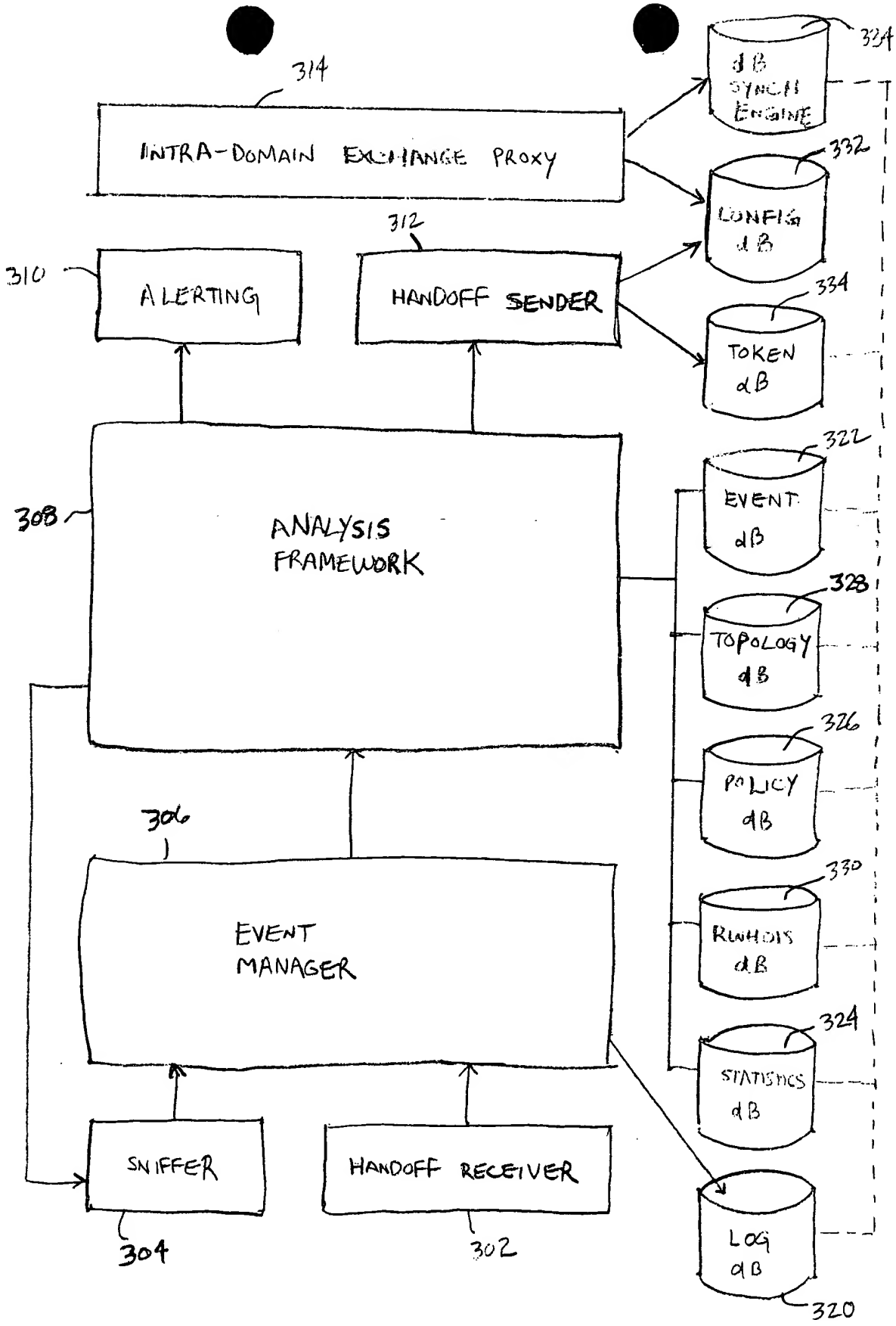
314
INTRA-DOMAIN EXCHANGE PROXY
312
310
ALERTING
HANDOFF SENDER
308
ANALYSIS FRAMEWORK
306
EVENT MANAGER
SNIFFER
HANDOFF RECEIVER
304
302
DB SYNCH ENGINE
324
CONFIG dB
332
TOKEN dB
334
EVENT dB
322
TOPOLOGY dB
328
POLICY dB
326
RWHOIS dB
330
STATISTICS dB
324
LOG dB
320

FIG. 3

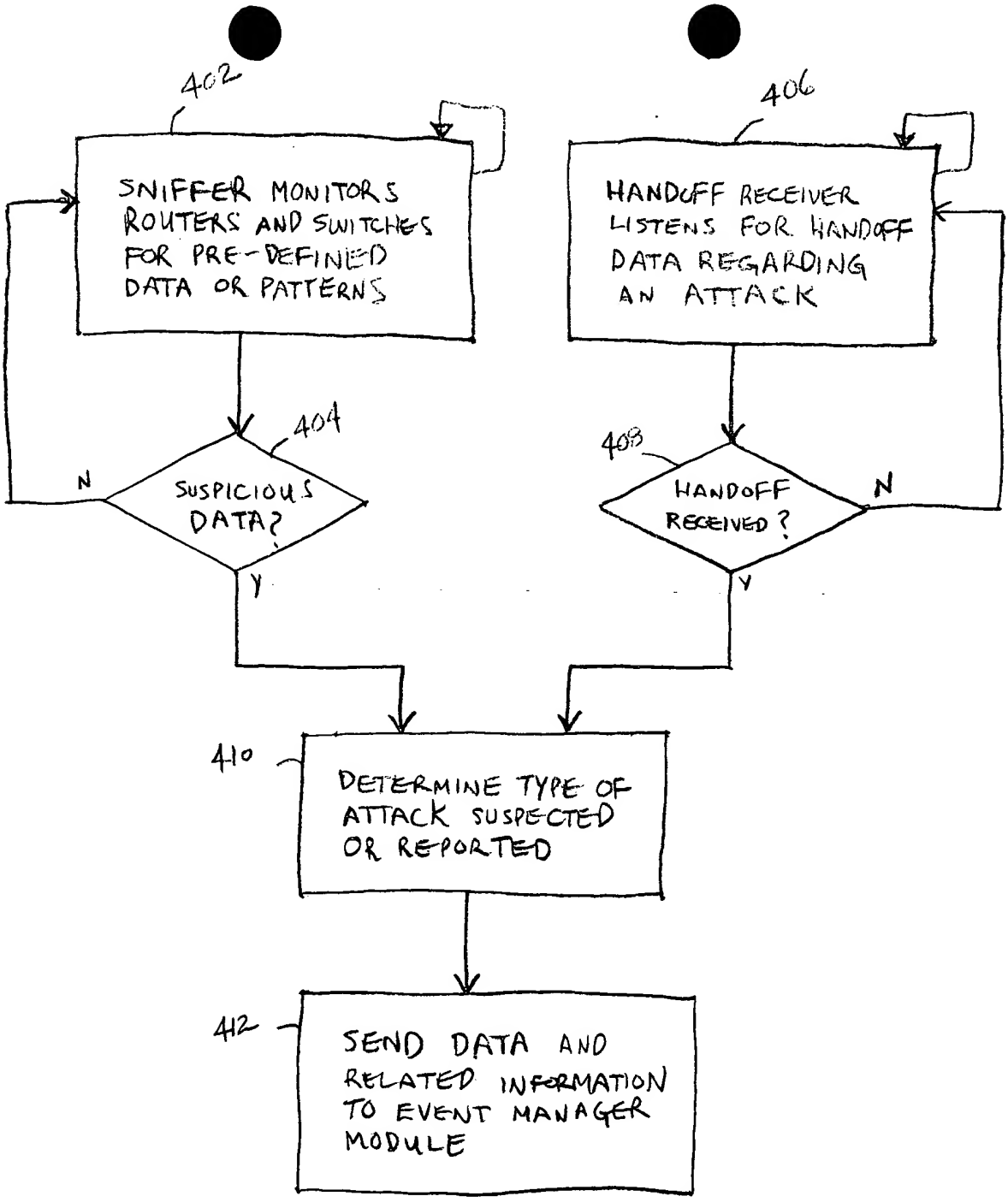
402
SNIFFER MONITORS ROUTERS AND SWITCHES FOR PRE-DEFINED DATA OR PATTERNS
404
SUSPICIOUS DATA?
N
Y
406
HANDOFF RECEIVER LISTENS FOR HANDOFF DATA REGARDING AN ATTACK
408
HANDOFF RECEIVED?
N
Y
410
DETERMINE TYPE OF ATTACK SUSPECTED OR REPORTED
412
SEND DATA AND RELATED INFORMATION TO EVENT MANAGER MODULE

FIG. 4

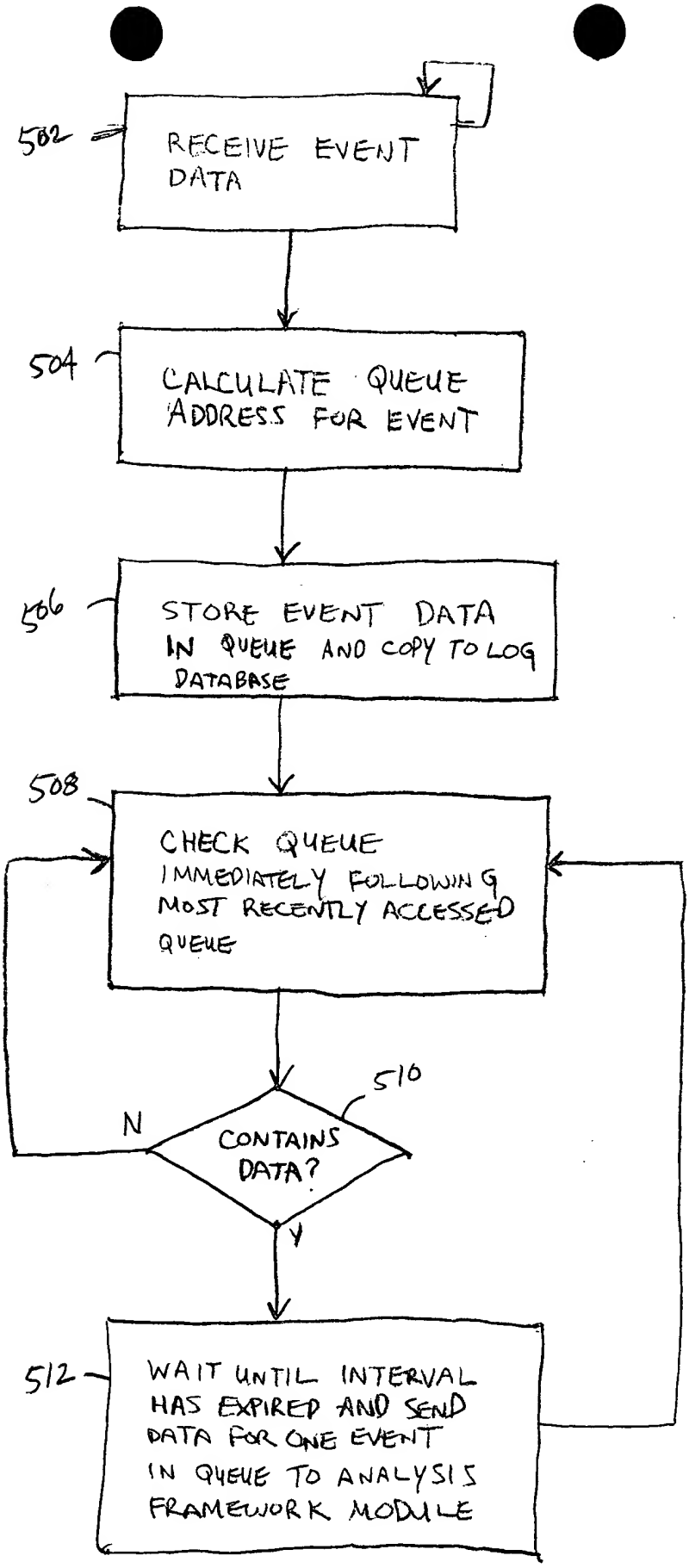
502
RECEIVE EVENT DATA
504
CALCULATE QUEUE ADDRESS FOR EVENT
506
STORE EVENT DATA IN QUEUE AND COPY TO LOG DATABASE
508
CHECK QUEUE IMMEDIATELY FOLLOWING MOST RECENTLY ACCESSED QUEUE
510
CONTAINS DATA?
N
Y
512
WAIT UNTIL INTERVAL HAS EXPIRED AND SEND DATA FOR ONE EVENT IN QUEUE TO ANALYSIS FRAMEWORK MODULE

FIG. 5

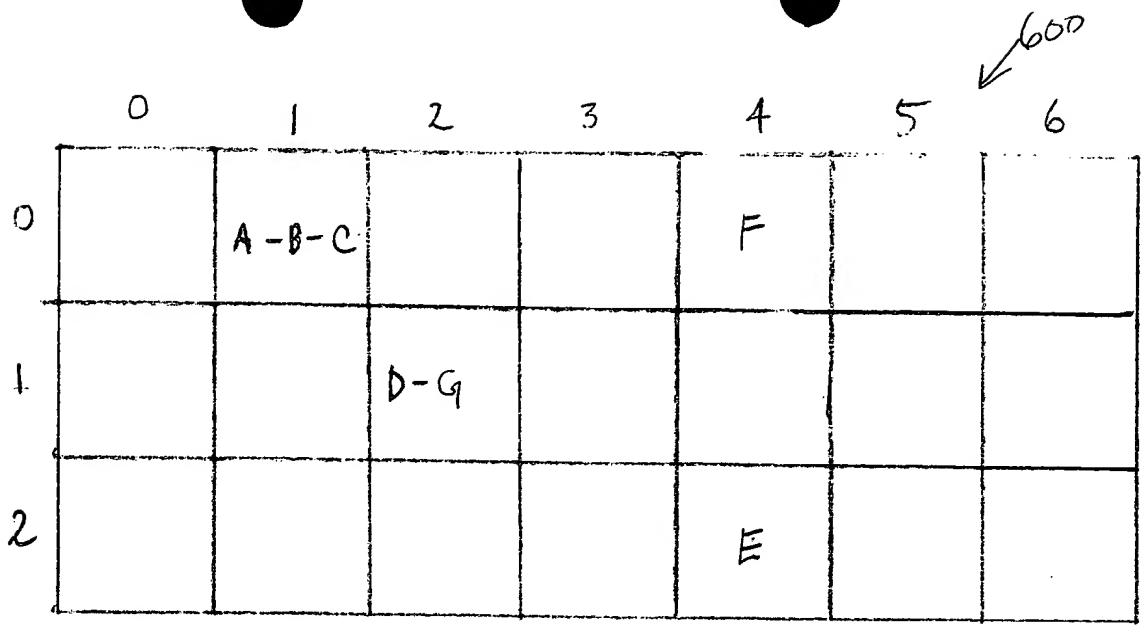

FIG. 6

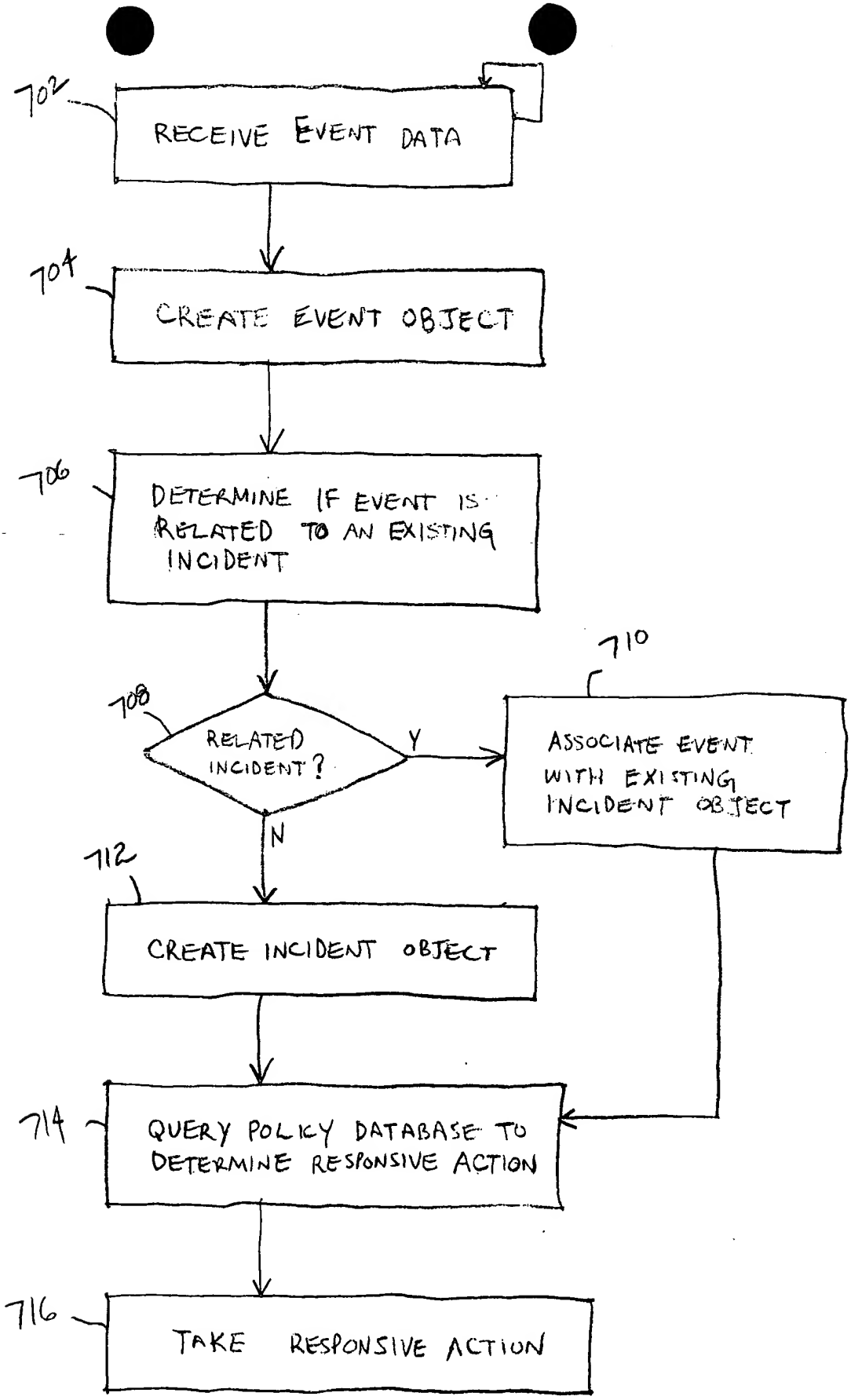
702
RECEIVE EVENT DATA
704
CREATE EVENT OBJECT
706
DETERMINE IF EVENT IS RELATED TO AN EXISTING INCIDENT
708
RELATED INCIDENT?
Y
N
710
ASSOCIATE EVENT WITH EXISTING INCIDENT OBJECT
712
CREATE INCIDENT OBJECT
714
QUERY POLICY DATABASE TO DETERMINE RESPONSIVE ACTION
716
TAKE RESPONSIVE ACTION

FIG. 7

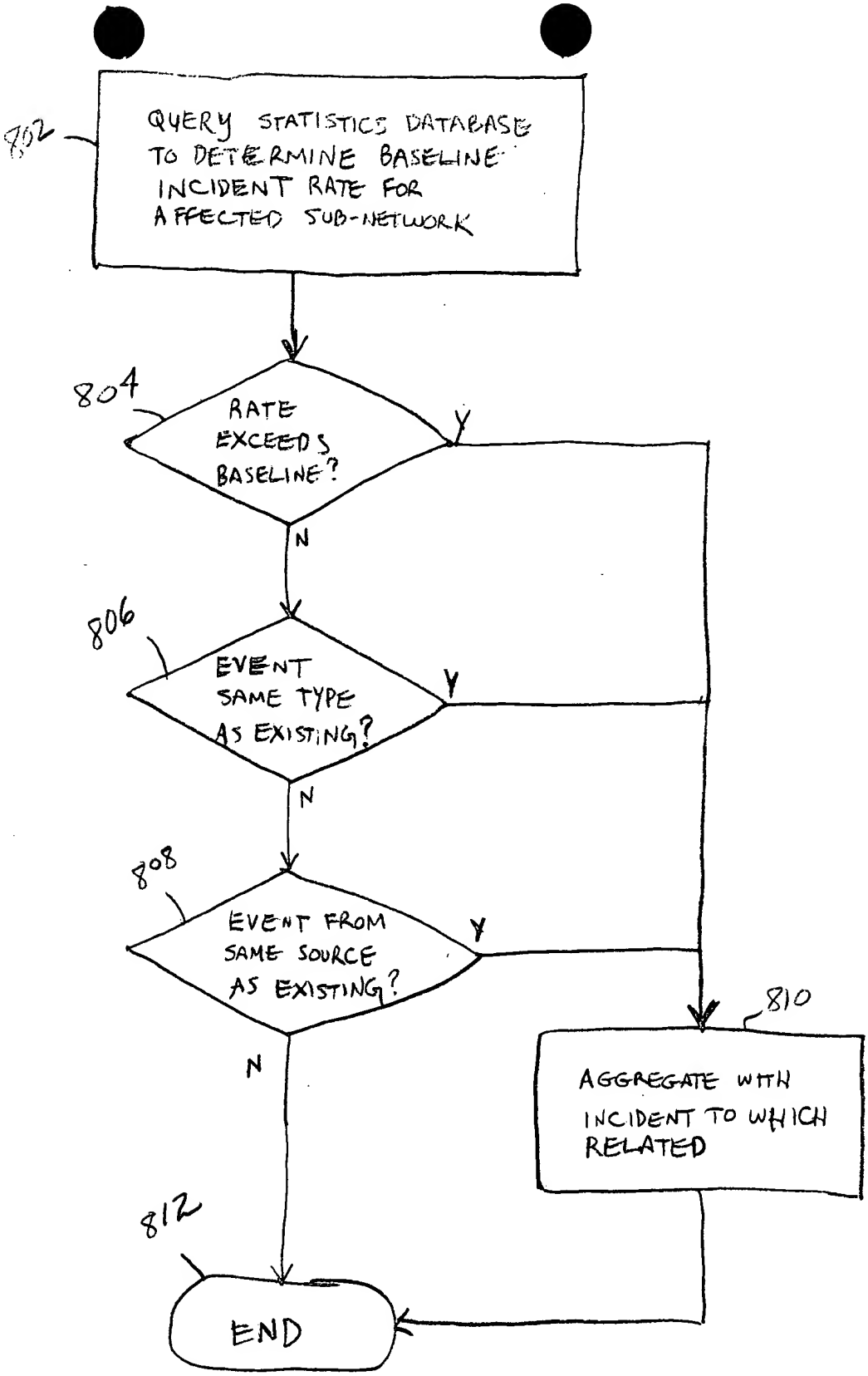
802
QUERY STATISTICS DATABASE TO DETERMINE BASELINE INCIDENT RATE FOR AFFECTED SUB-NETWORK
804
RATE EXCEEDS BASELINE?
Y
N
806
EVENT SAME TYPE AS EXISTING?
Y
N
808
EVENT FROM SAME SOURCE AS EXISTING?
Y
N
810
AGGREGATE WITH INCIDENT TO WHICH RELATED
812
END

FIG. 8

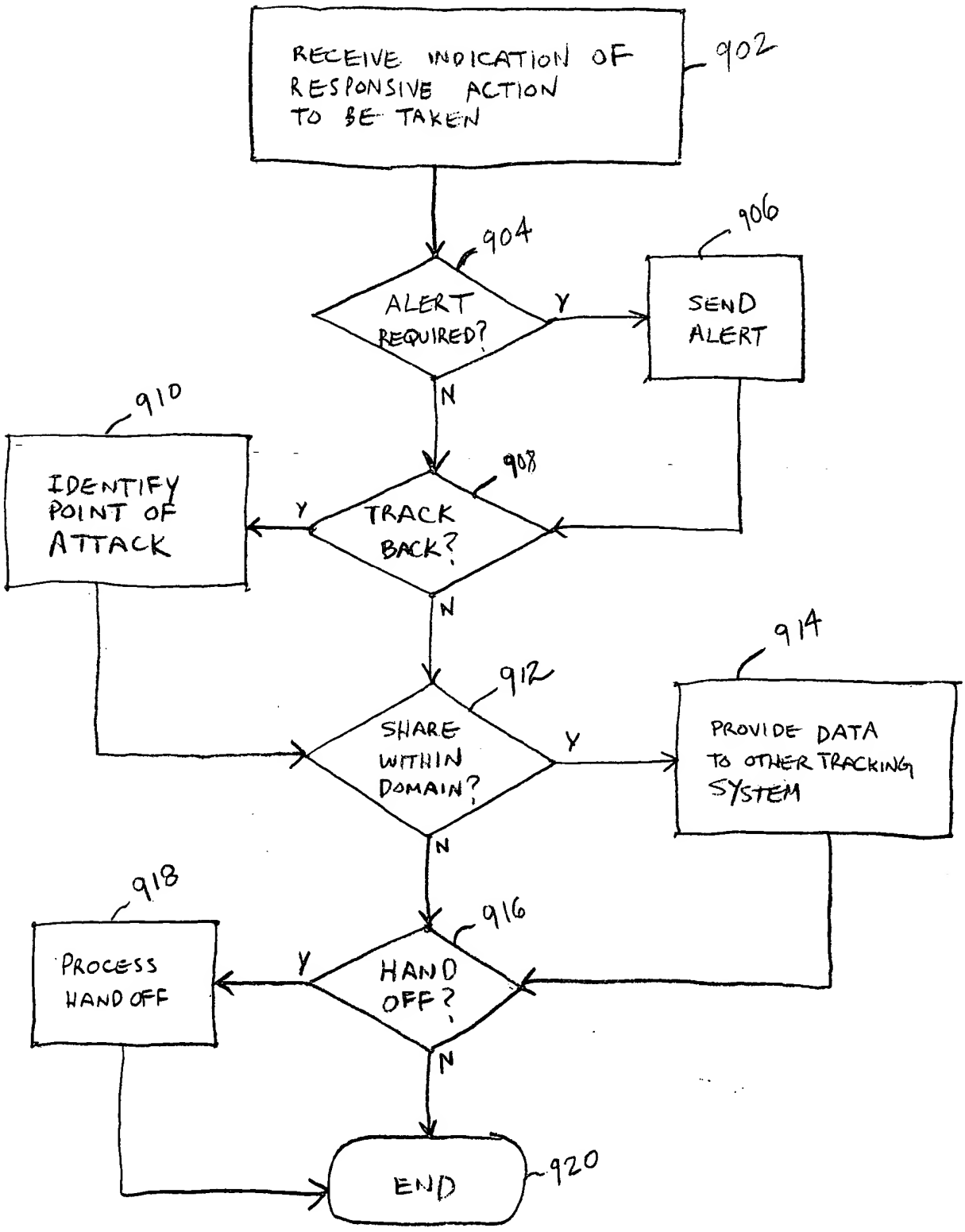
RECEIVE INDICATION OF RESPONSIVE ACTION TO BE TAKEN
902
ALERT REQUIRED?
904
Y
SEND ALERT
906
N
IDENTIFY POINT OF ATTACK
910
Y
TRACK BACK?
908
N
SHARE WITHIN DOMAIN?
912
Y
PROVIDE DATA TO OTHER TRACKING SYSTEM
914
N
PROCESS HAND OFF
918
Y
HAND OFF?
916
N
END
920

FIG. 9

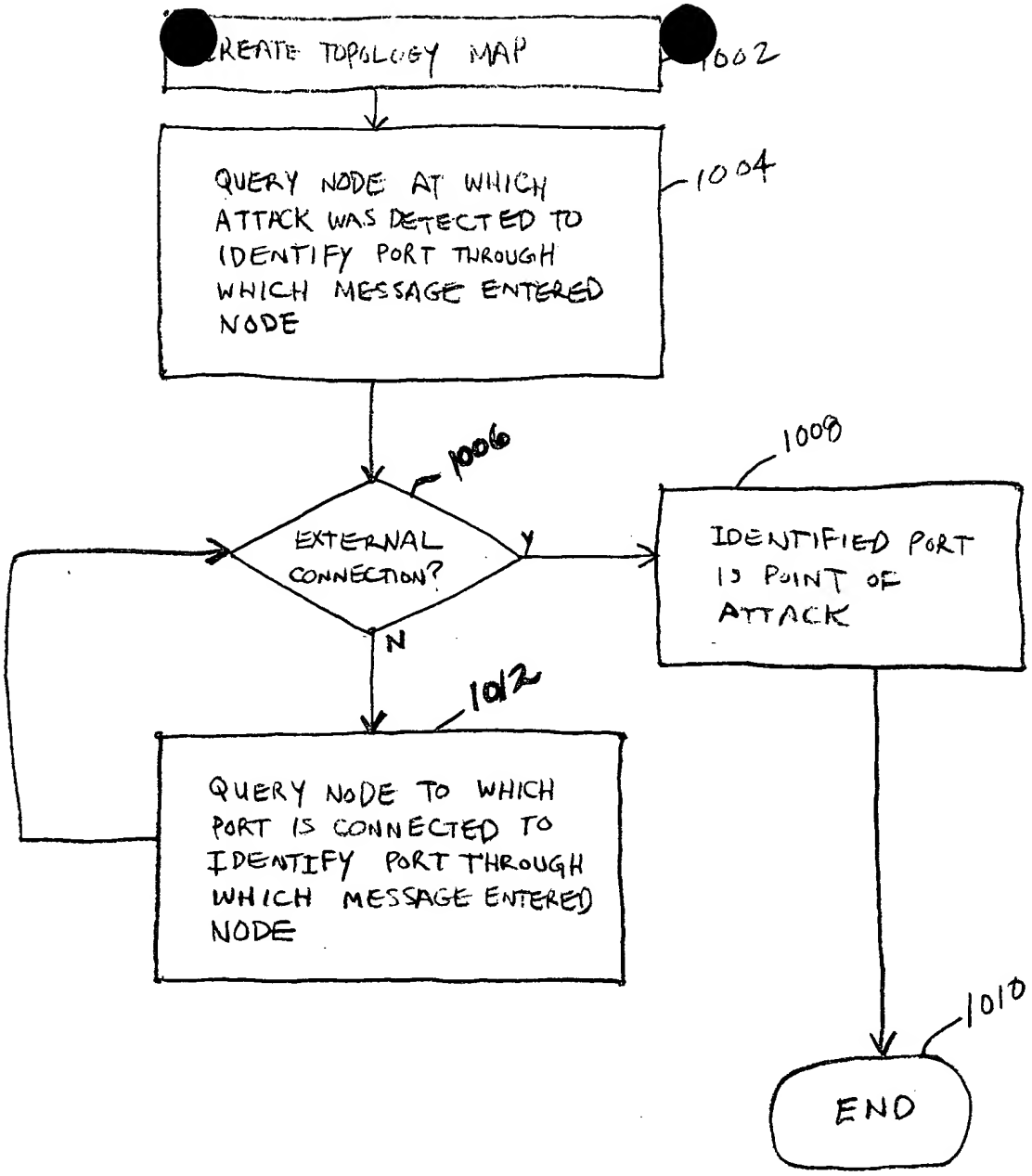
CREATE TOPOLOGY MAP
1002
QUERY NODE AT WHICH ATTACK WAS DETECTED TO IDENTIFY PORT THROUGH WHICH MESSAGE ENTERED NODE
1004
1006
EXTERNAL CONNECTION?
Y
N
1008
IDENTIFIED PORT IS POINT OF ATTACK
1012
QUERY NODE TO WHICH PORT IS CONNECTED TO IDENTIFY PORT THROUGH WHICH MESSAGE ENTERED NODE
1010
END

FIG. 10

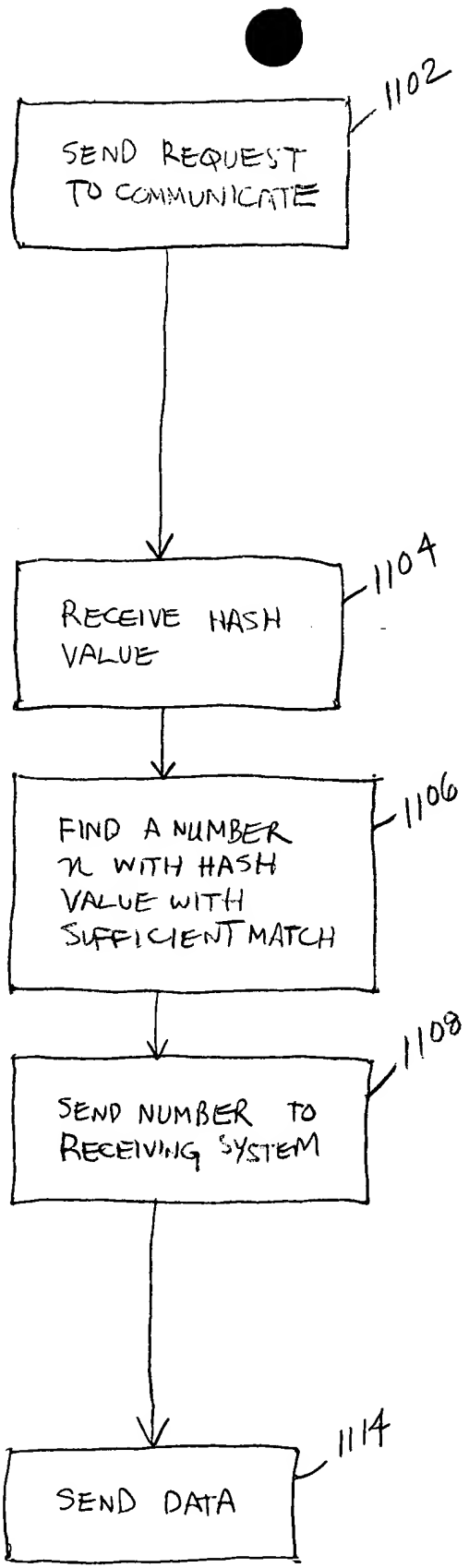

FIG. 11A

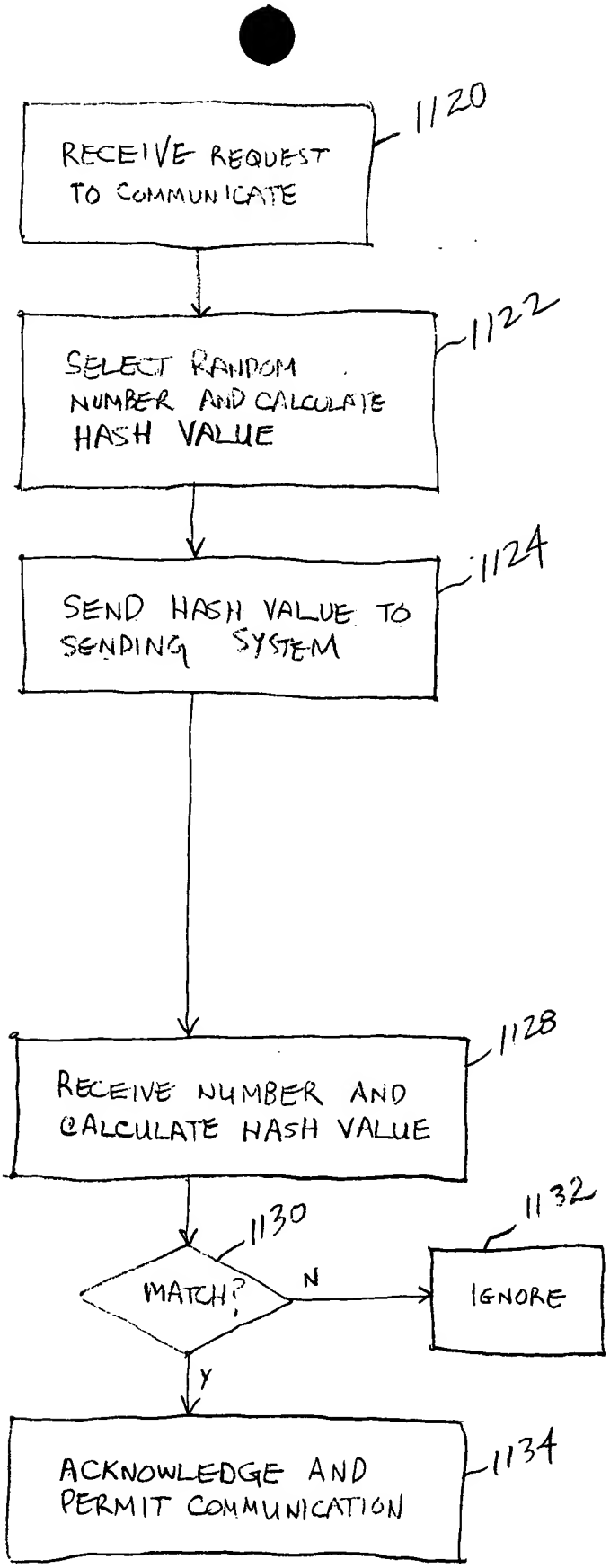

FIG. 11B

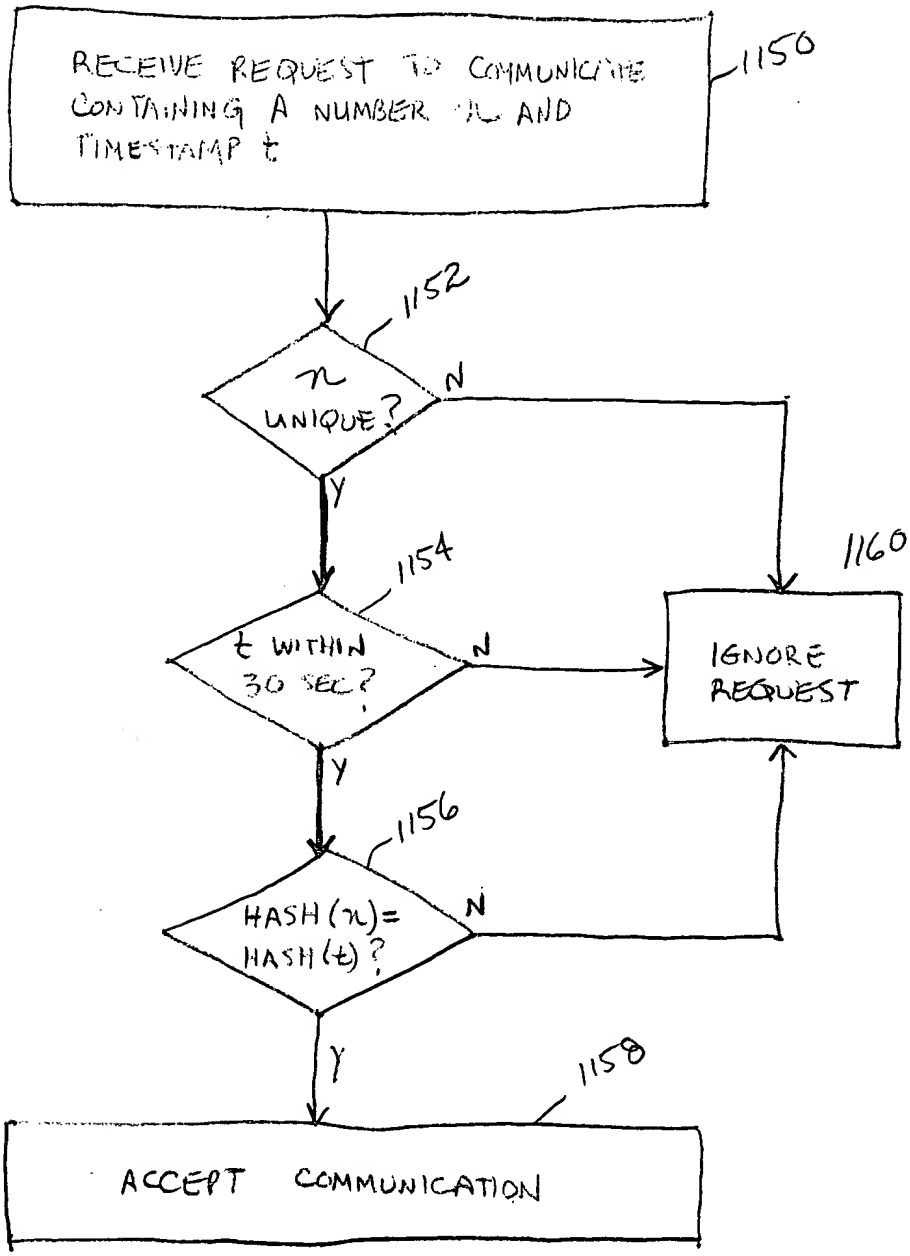
RECEIVE REQUEST TO COMMUNICATE CONTAINING A NUMBER n AND TIMESTAMP t
1150
1152
n UNIQUE?
N
Y
1154
t WITHIN 30 SEC?
N
1160
IGNORE REQUEST
Y
1156
HASH(n)= HASH(t)?
N
Y
1158
ACCEPT COMMUNICATION

FIG. 11C

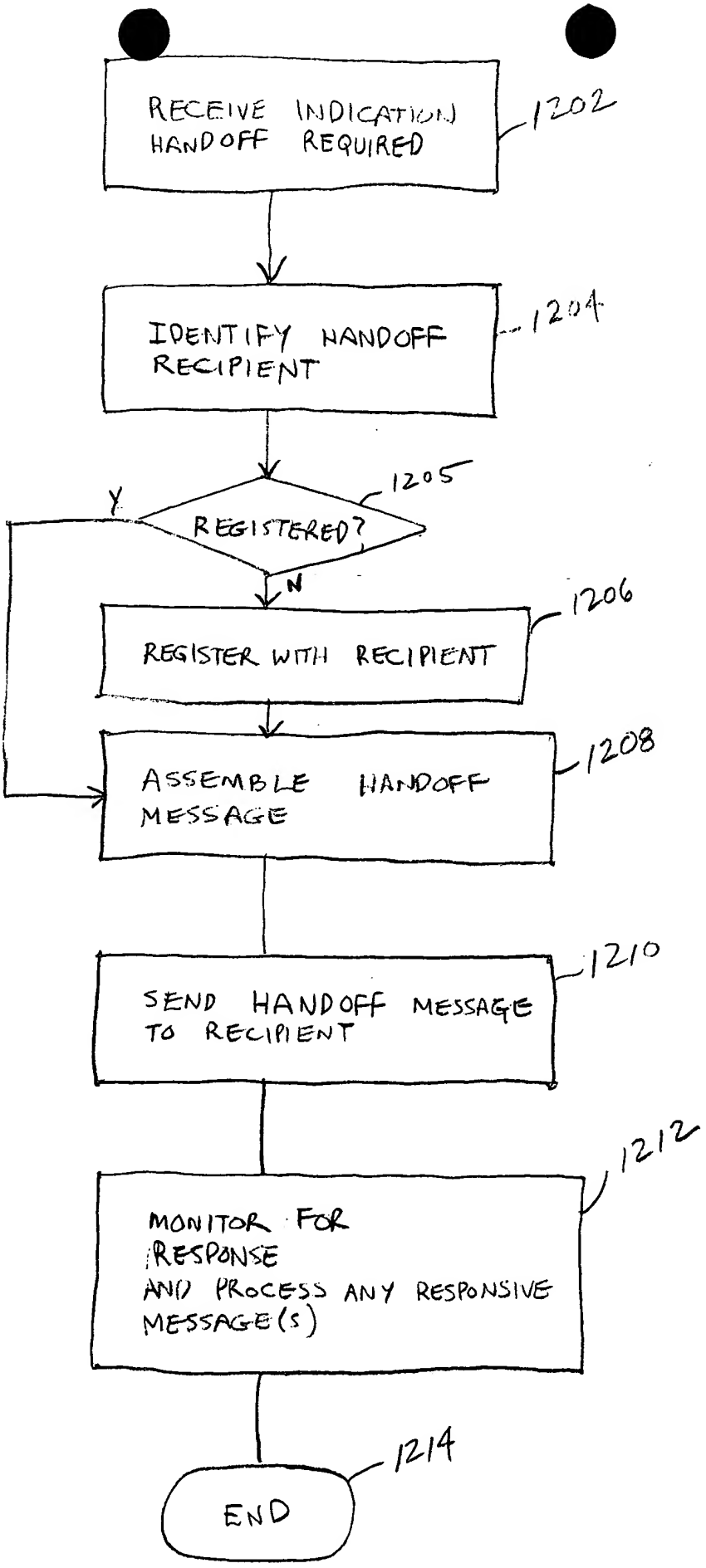
RECEIVE INDICATION HANDOFF REQUIRED
1202
IDENTIFY HANDOFF RECIPIENT
1204
REGISTERED?
1205
Y
N
REGISTER WITH RECIPIENT
1206
ASSEMBLE HANDOFF MESSAGE
1208
SEND HANDOFF MESSAGE TO RECIPIENT
1210
MONITOR FOR RESPONSE AND PROCESS ANY RESPONSIVE MESSAGE(S)
1212
END
1214

FIG. 12

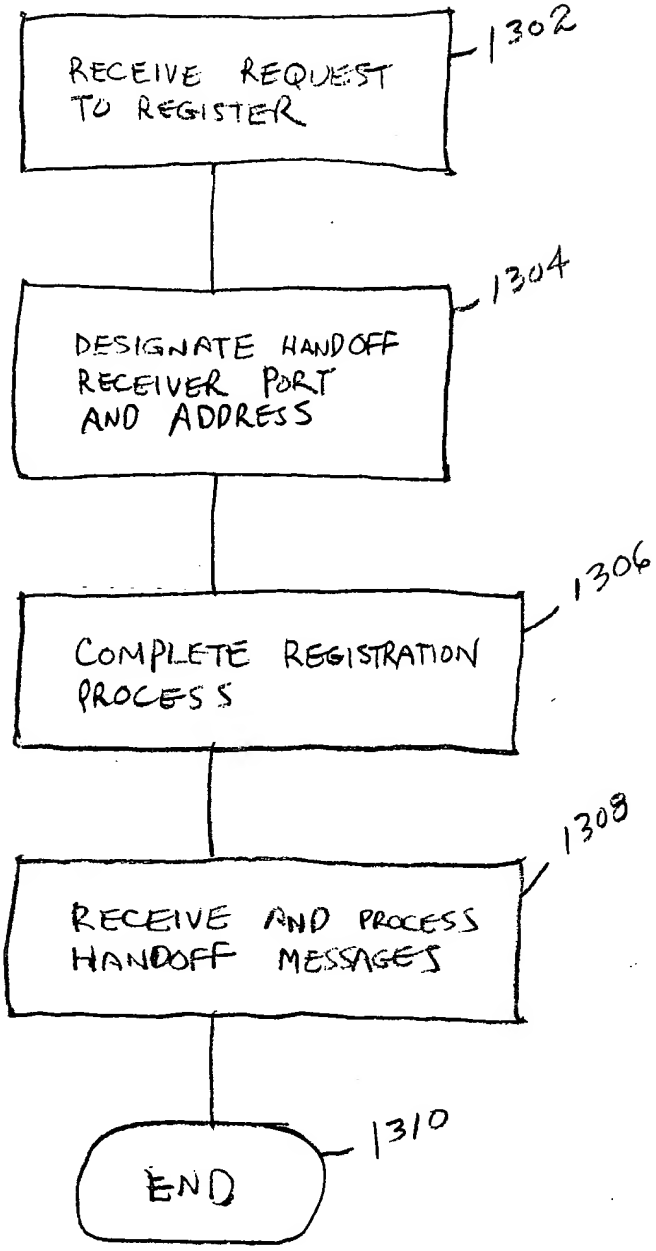
RECEIVE REQUEST TO REGISTER
1302
DESIGNATE HANDOFF RECEIVER PORT AND ADDRESS
1304
COMPLETE REGISTRATION PROCESS
1306
RECEIVE AND PROCESS HANDOFF MESSAGES
1308
END
1310

FIG. 13

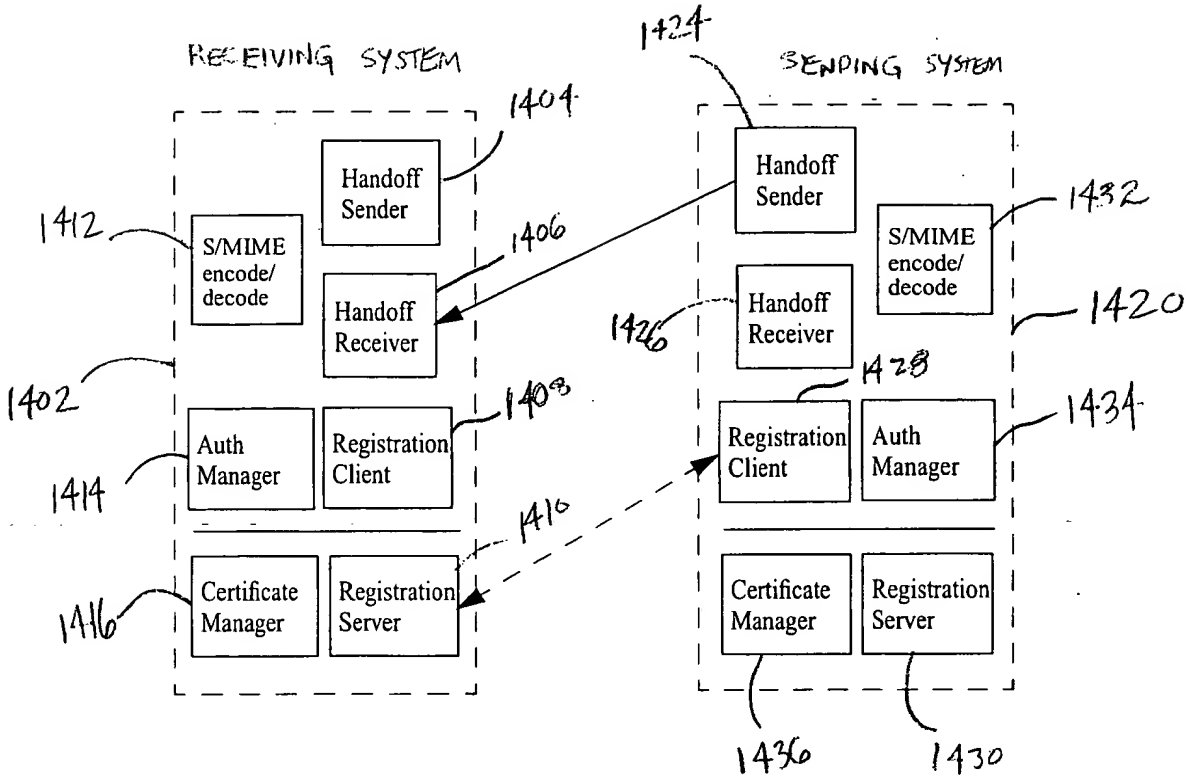
RECEIVING SYSTEM
SENDING SYSTEM
1424
1404
Handoff Sender
1412
S/MIME encode/ decode
1406
Handoff Receiver
1402
1408
Auth Manager
Registration Client
1414
1410
Certificate Manager
Registration Server
1416
Handoff Sender
1432
S/MIME encode/ decode
1420
1426
Handoff Receiver
1428
Registration Client
Auth Manager
1434
Certificate Manager
Registration Server
1436
1430

FIG. 14

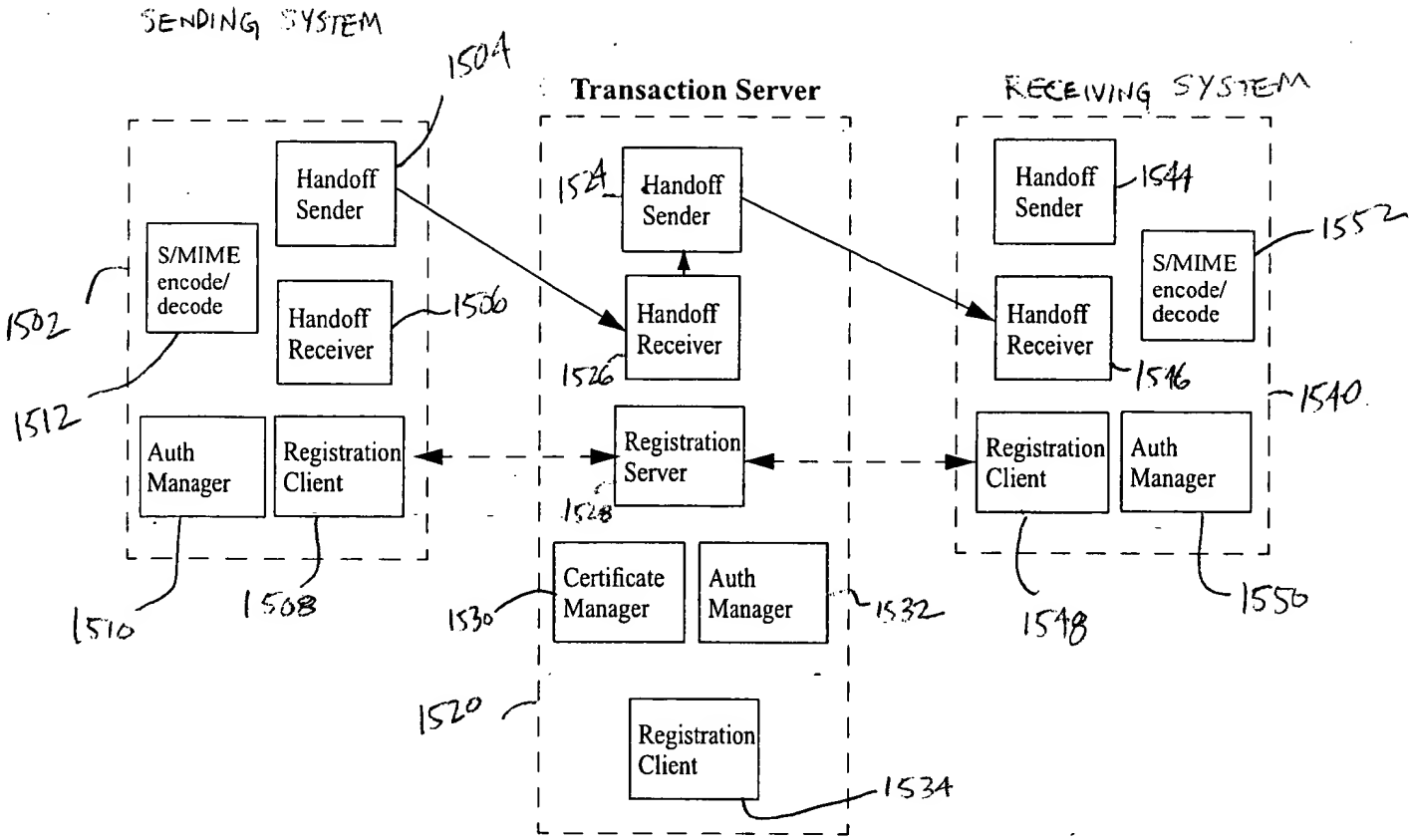
SENDING SYSTEM
1504
Transaction Server
RECEIVING SYSTEM
Handoff Sender
S/MIME encode/ decode
Handoff Receiver
Auth Manager
Registration Client
1502
1512
1506
1510
1508
1524
Handoff Sender
Handoff Receiver
Registration Server
1526
Certificate Manager
Auth Manager
1530
1532
1520
Registration Client
1534
Handoff Sender
1544
S/MIME encode/ decode
1552
Handoff Receiver
1546
1540
Registration Client
Auth Manager
1548
1550

FIG. 15

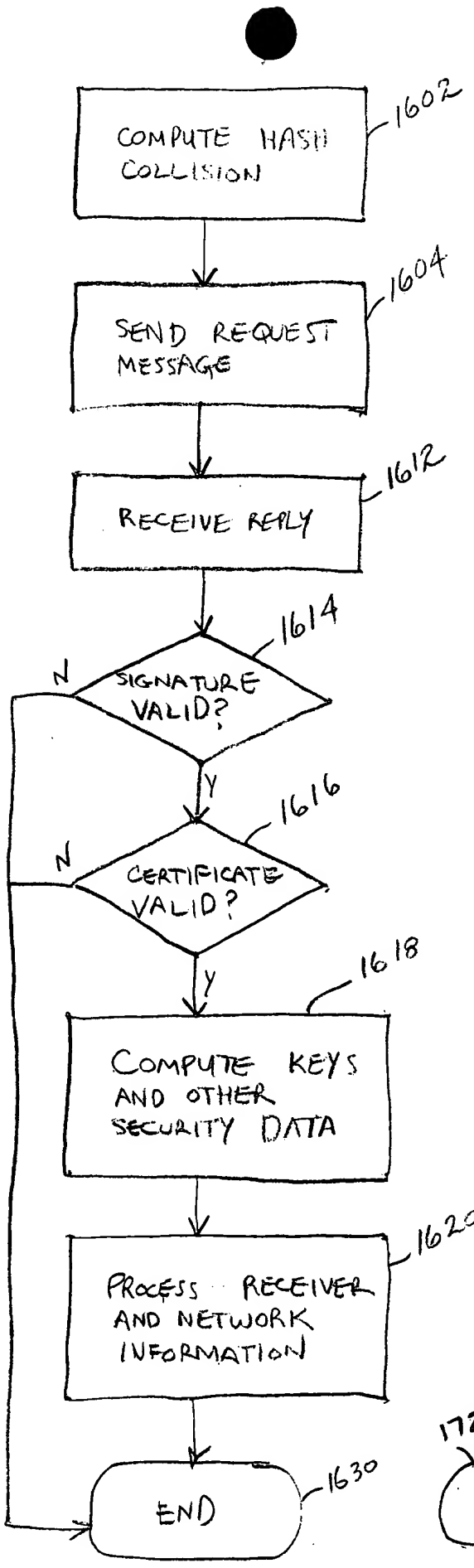
COMPUTE HASH COLLISION
1602
SEND REQUEST MESSAGE
1604
RECEIVE REPLY
1612
SIGNATURE VALID?
1614
N
Y
CERTIFICATE VALID?
1616
N
Y
COMPUTE KEYS AND OTHER SECURITY DATA
1618
PROCESS RECEIVER AND NETWORK INFORMATION
1620
END
1630

FIG. 16

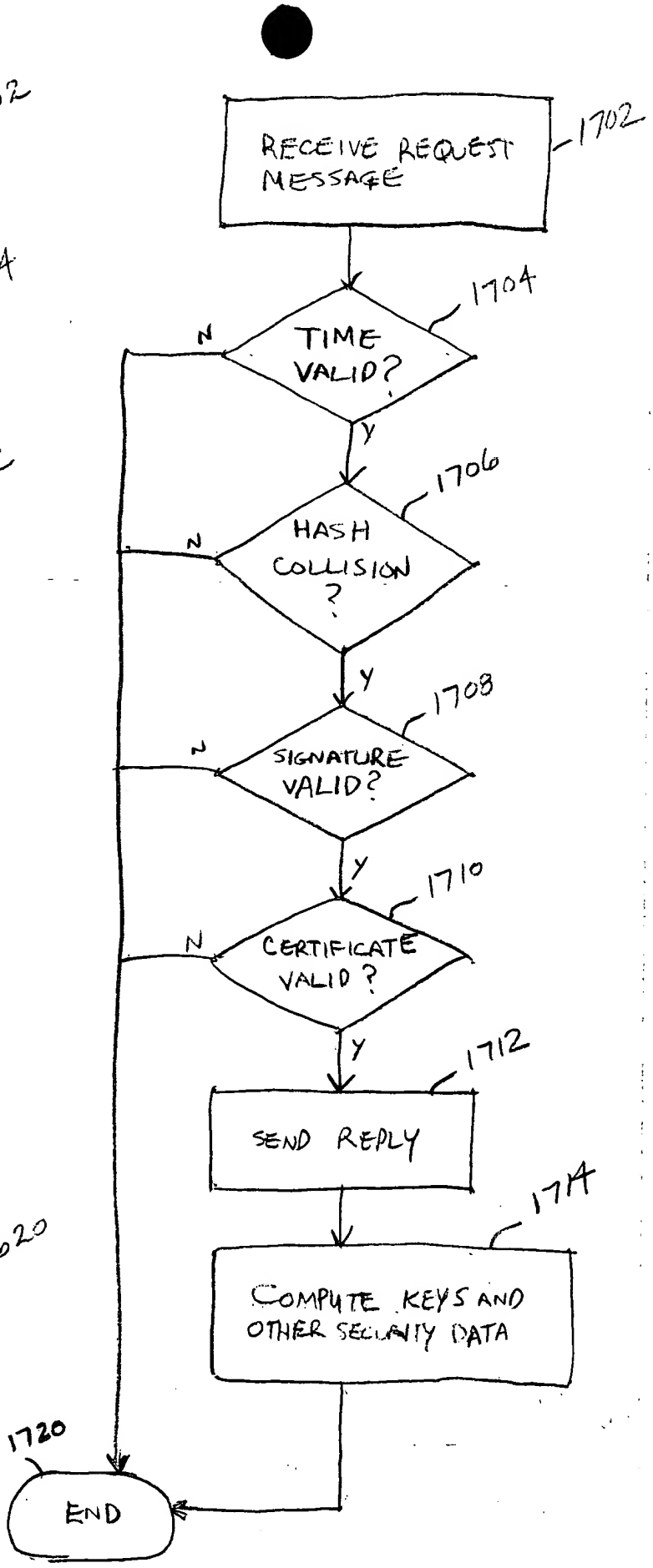
RECEIVE REQUEST MESSAGE
1702
TIME VALID?
1704
N
Y
HASH COLLISION ?
1706
N
Y
SIGNATURE VALID?
1708
N
Y
CERTIFICATE VALID ?
1710
N
Y
SEND REPLY
1712
COMPUTE KEYS AND OTHER SECURITY DATA
1714
END
1720

FIG. 17

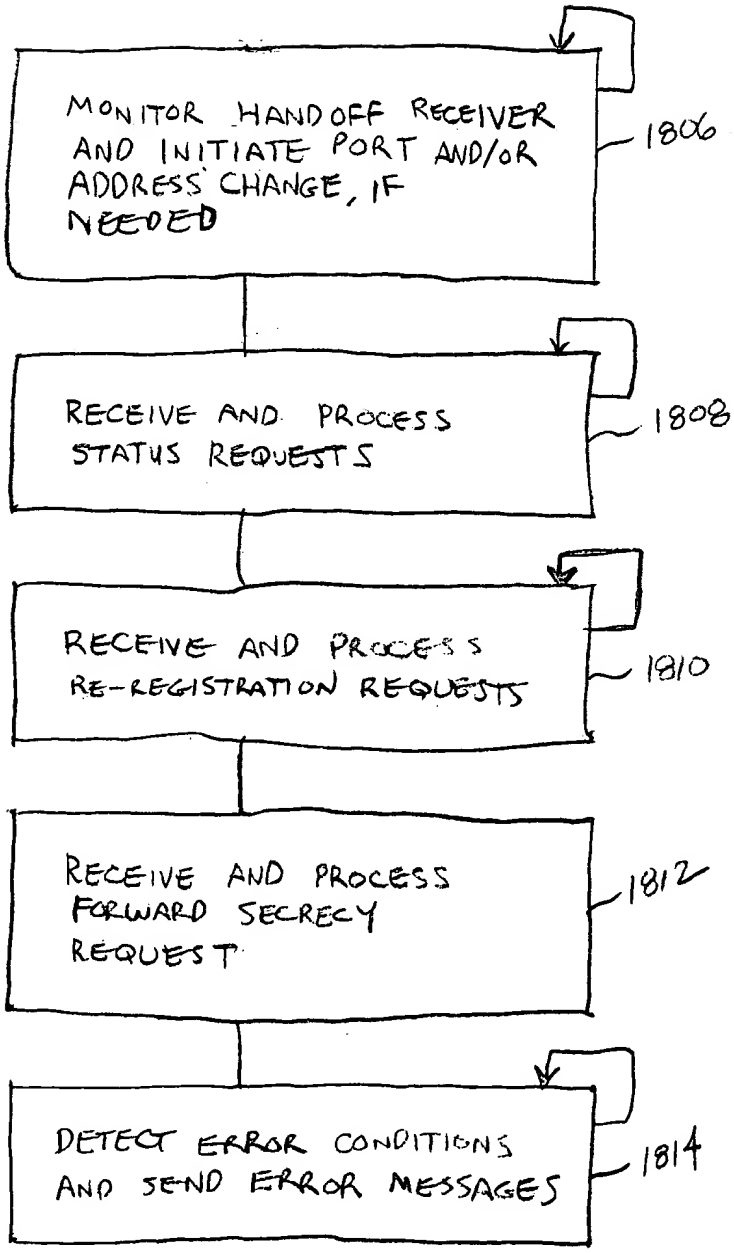
MONITOR HANDOFF RECEIVER AND INITIATE PORT AND/OR ADDRESS CHANGE, IF NEEDED
1806
RECEIVE AND PROCESS STATUS REQUESTS
1808
RECEIVE AND PROCESS RE-REGISTRATION REQUESTS
1810
RECEIVE AND PROCESS FORWARD SECRECY REQUEST
1812
DETECT ERROR CONDITIONS AND SEND ERROR MESSAGES
1814

FIG. 18

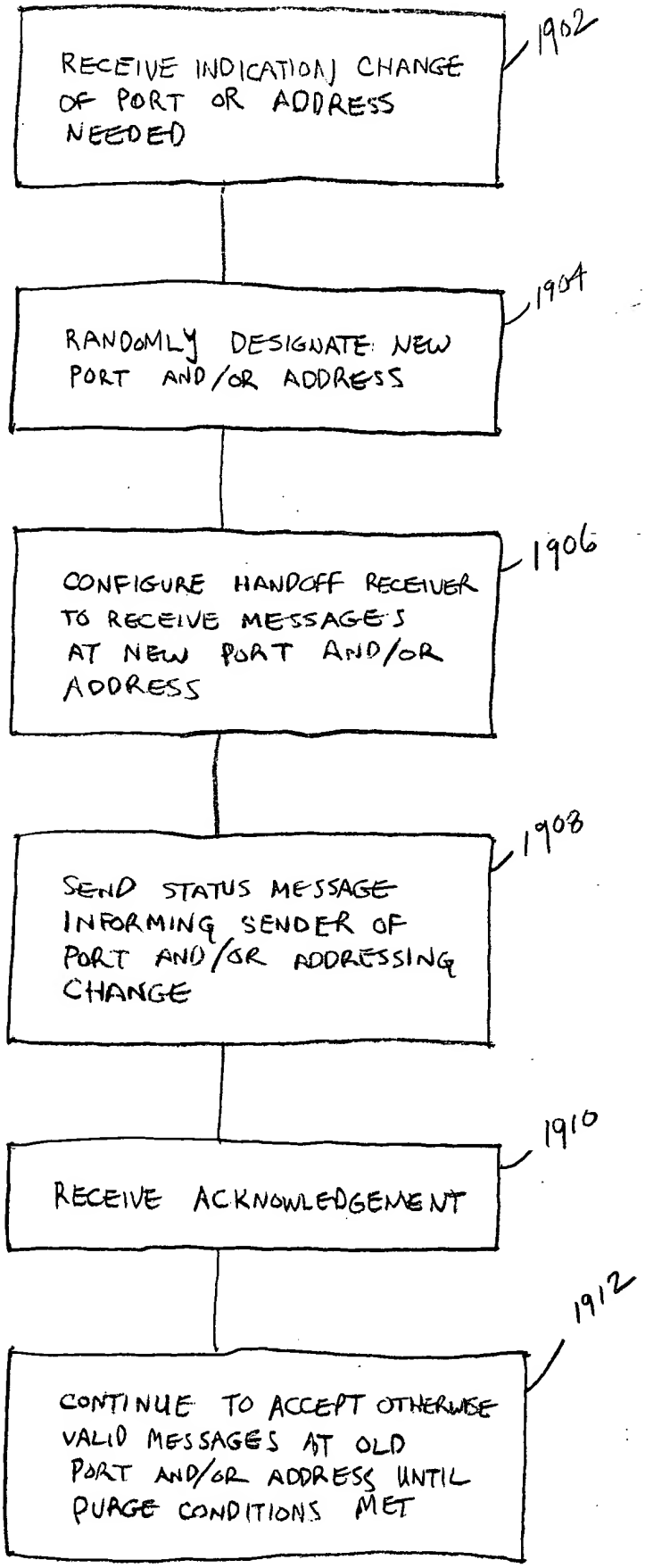
RECEIVE INDICATION CHANGE OF PORT OR ADDRESS NEEDED
1902
RANDOMLY DESIGNATE NEW PORT AND/OR ADDRESS
1904
CONFIGURE HANDOFF RECEIVER TO RECEIVE MESSAGES AT NEW PORT AND/OR ADDRESS
1906
SEND STATUS MESSAGE INFORMING SENDER OF PORT AND/OR ADDRESSING CHANGE
1908
RECEIVE ACKNOWLEDGEMENT
1910
CONTINUE TO ACCEPT OTHERWISE VALID MESSAGES AT OLD PORT AND/OR ADDRESS UNTIL PURGE CONDITIONS MET
1912

FIG. 19

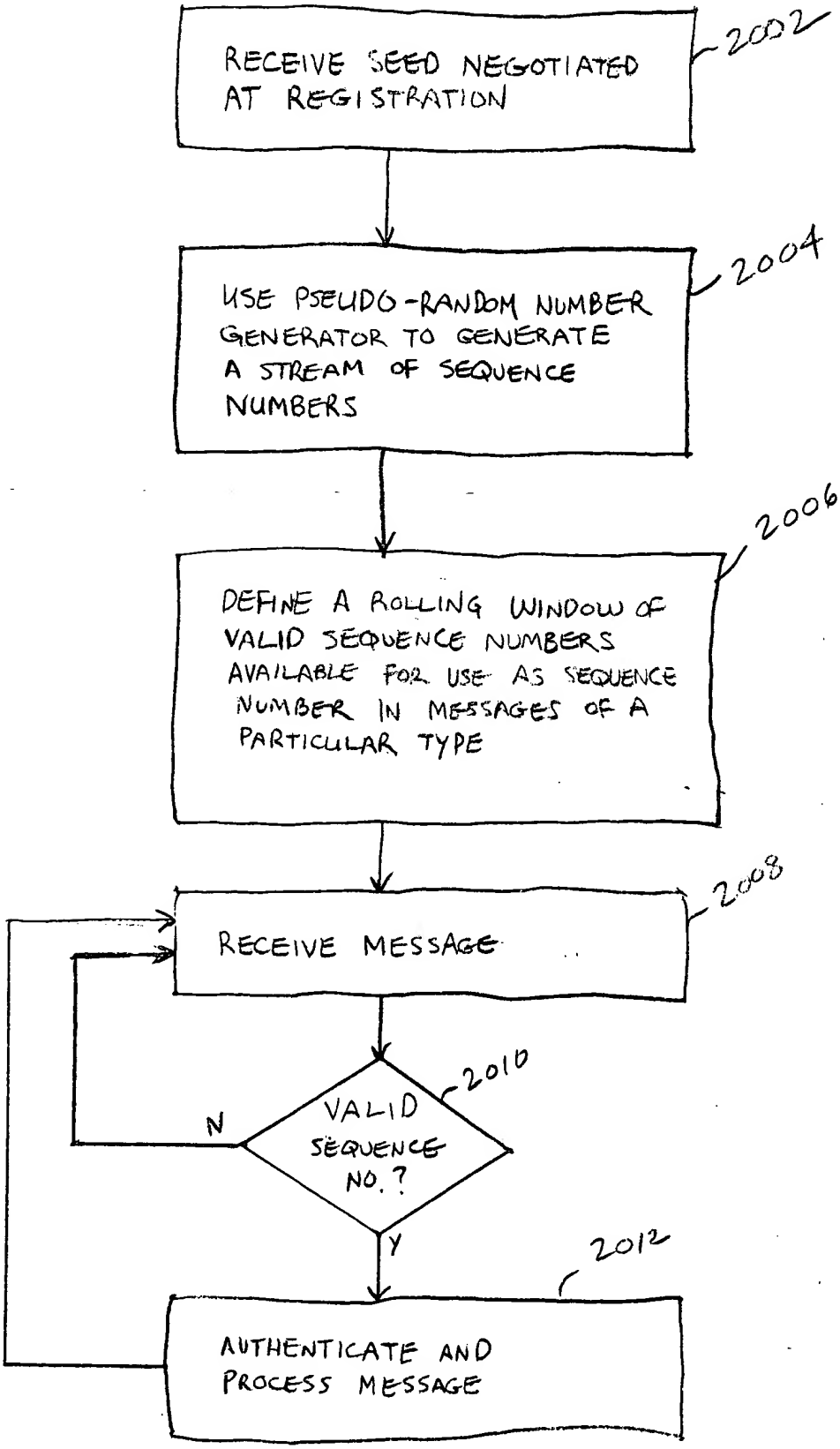
RECEIVE SEED NEGOTIATED AT REGISTRATION
2002
USE PSEUDO-RANDOM NUMBER GENERATOR TO GENERATE A STREAM OF SEQUENCE NUMBERS
2004
DEFINE A ROLLING WINDOW OF VALID SEQUENCE NUMBERS AVAILABLE FOR USE AS SEQUENCE NUMBER IN MESSAGES OF A PARTICULAR TYPE
2006
RECEIVE MESSAGE
2008
VALID SEQUENCE NO.?
2010
N
Y
AUTHENTICATE AND PROCESS MESSAGE
2012

FIG. 20